IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Microsoft Corporation,

Plaintiff,

v.

Does 1-10 Operating an Azure Abuse Network,

Defendants.

Civil Action No.

FILED UNDER SEAL

DECLARATION OF MAURICE MASON IN SUPPORT OF MICROSOFT'S MOTION FOR TEMPORARY RESTRAINING ORDER AND RELATED RELEIF

I, Maurice Mason, declare as follows:

1. I am a Principal investigator in Microsoft Corporation's Digital Crimes Unit ("DCU"). I respectfully submit this declaration in support of Microsoft's motion for an emergency *ex parte* temporary restraining order and order to show cause why a preliminary injunction should not be entered in the above-captioned case.

2. I make this declaration based upon my personal knowledge, and upon information and belief from my review of documents and evidence collected during Microsoft's investigation of the Azure Abuse Enterprise.

3. I have been employed by Microsoft since August 2021. In my role, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Among my responsibilities is protecting Microsoft's online service assets from network-based attacks. Prior to my current role, I worked as a Senior Consultant on Microsoft's Incident Response Team, where I was a lead digital forensic analyst managing multiple incident response and threat-hunting engagements that included performing incident response and

forensic analysis for Fortune 500, Fortune 100, and Fortune 50 companies. Prior to joining Microsoft, I held various positions, both in the private sector and in government, where I performed digital forensic analysis, including on malware and ransomware-related matters. A true and correct copy of my curriculum vitae is attached to this declaration as Exhibit 1.

4. Since in or about August 2024, I have been part of the team investigating the attack on Microsoft's systems by the Defendants referred to in the Complaint in this case as the Azure Abuse Enterprise. My role to date has included investigation of images generated as a result of the Azure Abuse Enterprise's attacks on Microsoft's system, including investigation of metadata contained in image files associated with the attack. My role has also included working with other investigators at Microsoft, including Jason Lyons and Rodelio Fiñones.

The Aitism.com Domain

5. Microsoft's investigation into the conduct described in the complaint led us to 4chan internet messages boards where the de3u software is being discussed. These message boards include discussion of prompt engineering tactics, images generated by misuse of Microsoft's tools, and links to domains that I understand can be used as pointers for directing de3u software.

6. One of the links provided in the 4chan messages boards I reviewed is to the URL "rentry.org/miniproxy". The website available at that URL contains a list of aitism.com subdomains. A true and correct screen capture of the list of aitism.com subdomain pointers provided on the rentry.org/miniproxy is attached to the Index of Evidence as Exhibit 6.

7. The rentry.org/miniproxy website also contains what purports to be user statistics for Defendants services.

C2PA Content Credentials

8. My work as an investigator requires me to have an understanding of digital forensic artifacts, including metadata. Metadata are information about data that describe the context, structure, format, origin, or other information about the data aside from their content.

9. One type of metadata relevant to my work in this case is a is a digitally signed manifest which contains a set of assertions commonly referred to as Coalition for Content Provenance and Authenticity ("C2PA") Content Credentials. Images generated by the Azure Abuse Enterprise contain C2PA Content Credentials.

10. C2PA Content Credentials are metadata generated by software specified by the Coalition for Content Provenance and Authenticity. C2PA is a Joint Development Foundation project that combats misleading information online by developing technical standards for certifying the provenance of media content.[1] Major technology and media companies, including Microsoft, Google, Adobe, BBC, and others, have aligned to develop the C2PA Specification, a standard for binding provenance information to pieces of media as "Content Credentials." Such provenance information may include data about a piece of content, such as the publisher or creator's information, where and when it was created, what tools were used to make it, including whether or not generative AI was used, as well as any edits that were made along the way.[2]

11. Microsoft, Google, Adobe, BBC, and others, have aligned to develop the C2PA Specification, a standard for binding provenance information to digital assets such AI generated

[1] See https://c2pa.org/.
[2] See https://c2pa.org/.

content, photos and videos. This provenance is stored as digitally signed manifests. The manifests are embedded as meta tags and act like nutrition labels for content. A nutrition label provides key information about food products such as ingredients, origin, and nutritional value. A C2PA manifest provides digitally signed data such as a unique identifier called a UUID, the date the content was created and most important a claim generator which labels the digital asset with the service that created the content. For example, one claim generator assertion for Microsoft products is 'Microsoft_Responsible_AI/1.0'. Another is 'Microsoft_Designer/1.0'

12. According to C2PA's website, the C2PA Specification's overarching goals serve creators, distributors, and consumers of online media by presenting a standardized method of authenticity and provenance chain verification. The C2PA Specification was developed with two overarching goals in mind. The first is providing "a mechanism for the producers and custodians of any given content to assert, in a verifiable manner, any information they wish to disclose about the creation of that content and any actions taken since the asset's creation."[3] The second goal is to provide that mechanism without also providing "value judgments about whether a given set of provenance data is 'good' or 'bad,' merely whether the assertions included within can be verified as associated with the underlying asset, correctly formed, and free from tampering."[4] To encourage widespread adoption and ease of use, The C2PA Specification is designed to allow implementations that mesh easily with existing infrastructure for creating, modifying, distributing, and consuming online media.

13. Metadata meeting the C2PA Specification include the original piece of media, its provenance information, and a digital signature. These metadata are cryptographically sealed into a tamper-evident "Manifest" that is bound to the piece of media. When a piece of media,

[3] https://c2pa.org/principles/
[4] https://c2pa.org/principles/

such as an image, with a C2PA manifest is edited, metadata regarding the edits are converted into a "New Assertion," which is digitally signed and added to the Manifest as part of the image's "Provenance Chain."[5] When users use editing and sharing tools that have not been tampered with, a piece of media's C2PA Content Credentials remain an accurate reflection of its Provenance Chain.

14. Images with metadata that meet the C2PA Specification are marked with a Content Credentials symbol ("CR Icon") that looks like a lowercase "CR" in a curved bubble which is made visible when a user interacts with the image. A user can access the image's C2PA Content Credentials by clicking on the CR Icon. The user is then presented with the image's full Provenance Chain and is able to determine its origin and any changes that have been made to the image.

15. When an image with C2PA Content Credentials has a corrupted or incomplete Manifest, the image's CR Icon appears yellow. The yellow CR Icon alerts users as to the risk of misleading or corrupted media without impeding consumption.

C2PA Content Credentials and Defendants Malicious Images

16. Microsoft is a C2PA founding member interested in facilitating the proliferation of online media in a way that allows users to make educated decisions about the content they modify and consume. For this reason, the Azure OpenAI Service includes an implementation of the C2PA Specification.

17. When users create images with Azure OpenAI Service, those images are cryptographically sealed with Manifests detailing their full Provenance Chain in accordance with the C2PA Specification. For this reason, images created with Azure OpenAI Service include CR

[5] See https://c2pa.org/.

Icons allowing users to determine those images' provenance information, including the fact that they originated within the Azure OpenAI Service. Included in the metadata accompanying the CR Icons is a metadata field containing Microsoft's Azure® registered trademark.

18. When Defendants abuse Azure OpenAI Service while executing the Azure Abuse Enterprise, the images they create are C2PA Specified and include Manifests detailing their full Provenance Chains. I understand that images containing C2PA Content Credentials are copied to infrastructure created by the Azure Abuse Enterprise, including at least a proxy server that is physically located within the Eastern District of Virginia. I have reviewed metadata for certain images created by the Azure Abuse Enterprise and confirmed that they contain C2PA Content Credentials identifying the Azure OpenAI Service as the source of the images.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge, information, and belief. Executed this 19th day of December, 2025 at Alexandria, Virginia.

Maurice Mason